



(11) **EP 1 605 626 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention
of the grant of the patent:
26.12.2007 Bulletin 2007/52

(51) Int Cl.:
H04L 9/30 (2006.01) H04L 29/06 (2006.01)

(21) Application number: **05104894.0**

(22) Date of filing: **06.06.2005**

(54) **Cryptographic method and apparatus**

Kryptografisches Verfahren und Gerät

Procédé et appareil cryptographique

(84) Designated Contracting States:
DE FR GB

(30) Priority: **11.06.2004 GB 0413056**

(43) Date of publication of application:
14.12.2005 Bulletin 2005/50

(73) Proprietor: **Hewlett-Packard Development
Company, L.P.
Houston, TX 77070 (US)**

(72) Inventors:
• **Harrison, Keith Alexander
Stoke Gifford
Bristol BS 34 8QZ (GB)**

• **Chen, Liquan
Stoke Gifford
Bristol BS34 8QZ (GB)**

(74) Representative: **Squibbs, Robert Francis et al
Hewlett-Packard Limited,
IP Section, Building 3
Filton Road
Stoke Gifford,
Bristol BS 34 8QZ (GB)**

(56) References cited:
GB-A- 2 395 872 US-A1- 2003 095 661
US-B1- 6 275 936

EP 1 605 626 B1

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

DescriptionField of the Invention

[0001] The present invention relates to a cryptographic method and apparatus; in particular, the present invention relates to an identifier-based cryptographic method and apparatus.

[0002] As is well known to persons skilled in the art, in "identifier-based" cryptographic methods the encryption key used to encrypt a message is based on a sender-chosen string and public data, the corresponding decryption key being computed, potentially subsequent to message encryption, using the sender-chosen string and private data associated with the public data. Frequently, the sender-chosen string serves to "identify" the intended message recipient and this has given rise to the use of the label "identifier-based" or "identity-based" generally for these cryptographic methods. However, depending on the application to which such a cryptographic method is put, the sender-chosen string may serve a different purpose to that of identifying the intended recipient and, indeed, may be an arbitrary string having no other purpose than to form the basis of the encryption key. Accordingly, the use of the term "identifier-based" herein in relation to cryptographic methods and apparatus is to be understood simply as implying that the encryption key is based on a sender-chosen, cryptographically unconstrained, string whether or not the string serves to identify the intended recipient, and that the corresponding decryption key can be subsequently computed from the string. Furthermore, as used herein the term "string" is simply intended to imply an ordered series of bits whether derived from a character string, a serialized image bit map, a digitized sound signal, or any other data source.

Background of the Invention

[0003] Identifier-Based Encryption (IBE) is an emerging cryptographic schema. A number of IBE cryptographic methods are known, including:

- methods based on "Quadratic Residuosity" as described in the paper: "An identity based encryption scheme based on quadratic residues", C. Cocks, Proceedings of the 8th IMA International Conference on Cryptography and Coding, LNCS 2260, pp 360-363, Springer-Verlag, 2001;
- methods using Weil or Tate pairings - see, for example: D. Boneh, M. Franklin - "Identity-based Encryption from the Weil Pairing" in Advances in Cryptology - CRYPTO 2001, LNCS 2139, pp. 213-229, Springer-Verlag, 2001;
- methods based on mediated RSA as described in the paper "Identity based encryption using mediated RSA", D. Boneh, X. Ding and G. Tsudik, 3rd Workshop on Information Security Application, Jeju Island, Korea, Aug, 2002.

[0004] Generally, in IB encryption/decryption methods, a trusted party carries out one or more actions (such as identity checking) in accordance with information in the sender-chosen string, before enabling a recipient to recover a message encrypted by a message sender. Usually, the trusted party will generate an IB decryption key and provide it to the recipient for the latter to use in decrypting the encrypted message. However, it is also possible to provide IB encryption/decryption methods in which the trusted party must itself carry out the decryption since it involves knowledge of a secret belonging to the trusted party as well as use of the IB decryption key. This is the case for the RSA-based IB method described in US patent 6,275,936 where the decryption exponent is dynamically computed from the encryption exponent, the latter being a hash of the sender-chosen string. A potential disadvantage of the trusted party carrying out message decryption is that it risks compromising the recipient's privacy. In the afore-mentioned US patent, this potential disadvantage is overcome by the recipient blinding the encrypted message before passing it to the trusted party (a decryption box) and then un-blinding the returned decrypted, but still blinded, message.

[0005] Document WO 03/063410 describes a cryptosystem in which users send and receive messages with the help of a trusted third party for security purposes making use of private keys and public parameters which encapsulate said private keys, each user holding a private key and the trusted third party being entrusted with a corresponding private key for each user, and the trusted third party being adapted so that it is responsive to a challenge from a user by issuing a response which encapsulates the corresponding private key so that the user can use the response in combination with the private key already held by the user to decrypt or sign a message.

[0006] It is an object of the present invention to provide novel identifier-based cryptographic methods and systems.

Summary of the Invention

[0007] According to a first aspect of the present invention, there is provided a cryptographic method in which a sender encrypts and sends a message to a recipient for decryption by a trusted party, the sender being in possession of a public key for which there exists a corresponding private key held by the trusted party, the method comprising:

the sender modifying the public key by exponentiating at least one element of that key using as exponent a hash of a string that comprises information concerning at least one action to be taken by the second party, and using the modified public key to encrypt said message;
the recipient receiving the encrypted message and said string and passing them to the trusted party; and
the trusted party using said string to modify its private key to compliment the modified public key, decrypting the message with the modified private key, and returning the decrypted message to the recipient after carrying out said at least one action with a satisfactory conclusion..

[0008] In preferred embodiments of the invention, the foregoing method is used to provide an identifier-based form of the ElGamal encryption/decryption system. The ElGamal cryptosystem is described in the paper: "A public key cryptosystem and a signature scheme based on discrete logarithms" (IEEE Transactions on Information Theory, Vol. IT-31 No.4 July 1985, Taher ElGamal) and is itself based on the well-known Diffie-Hellman key distribution scheme.

[0009] The identifier-based encryption/decryption methods provided by preferred embodiments of the present invention present a different distribution of computational load to other identifier-based systems (such as the RSA-based system described in the above-referenced US patent) and in appropriate circumstances offers performance advantages over the prior art.

[0010] According to a second aspect of the present invention, there is provided a cryptographic method, wherein a trusted party with secret x and public parameters p and g , effects at least steps of:

receiving values h and J and a condition string STR from a message sender, the condition string comprising at least one condition to be checked by the trusted party;
computing:

$z \leftarrow \#(STR)$, where $\#$ is a hash function;

computing:

$$f^{-1}(J, h^{z \cdot x})$$

where $f^{-1}()$ inverts an invertible operation $f()$, whereby to produce a result which corresponds to a decrypted message m when:

the received value of h corresponds to $g^r \bmod p$ where r is a secret belonging to the sender (A), and
the received value of J corresponds to $f(g^{r \cdot x \cdot z}, m)$;

the trusted party only computing said result, or only releasing the result, after confirming that said at least one condition contained in the string has been met.

[0011] According to a third aspect of the present invention, there is provided cryptographic apparatus comprising first, second and third computing entities, the first computing entity (A) comprising:

an input arrangement for receiving a public key for which there exists a corresponding private key held by the second computing entity,
a key-processing arrangement arranged to modify the public key by exponentiating at least one element of the received public key using as exponent a hash of a string, this string comprising information concerning at least one action to be taken by the second computing entity,
an encryption arrangement for encrypting a message using the modified public key; and
an output arrangement for outputting the encrypted message and said string;

the third computing entity being arranged to receive the encrypted message and the string and pass them to the second computing entity, and the second computing entity being arranged to receive message and the string, to use the string to modify its private key to compliment the modified public key, and to decrypt the message using the modified private key, the second computing entity being arranged to only decrypt the message, or only release the decrypted message, after carrying out said at least one action with a satisfactory conclusion.

[0012] According to a fourth aspect of the present invention, there is provided a trusted-party entity comprising:

a data store for storing a secret x and public parameters p and g ;

an input arrangement for receiving values h and J and a condition string STR from a message sender, the condition string comprising at least one condition to be checked by the trusted party;
 a processing arrangement arranged to compute:

$z \leftarrow \#(STR)$; and $f^1(J, h^{z \cdot x})$ where $f^1()$ inverts an invertible operation $f()$, whereby to produce a result which corresponds to a decrypted message m when:

the received value of h corresponds to $g^r \bmod p$ where r is a secret belonging to the sender, and
 the received value of J corresponds to $f(g^{r \cdot x \cdot z}, m)$;

an output arrangement for outputting said result; and
 a control arrangement arranged to check that said at least one condition contained in the string has been met, and only permit the processing arrangement to compute said result, or only permit said output arrangement to output said result, where said at least one condition has been met.

Brief Description of the Drawings

[0013] Embodiments of the invention will now be described, by way of non-limiting example, with reference to the accompanying diagrammatic drawings, in which:

- Figure 1 is a diagram illustrating the operational steps of the prior art ElGamal public key encryption/decryption method;
- Figure 2 is a diagram illustrating the operational steps of an identifier-based cryptographic method embodying the invention; and
- Figure 3 is a diagram similar to that of Figure 2 but illustrating the inclusion of addition blinding and un-blinding operational steps.

Best Mode of Carrying Out the Invention

[0014] The cryptographic methods and apparatus described below with respect to Figures 1 to 3 involve two or three parties, namely a message sender A acting through computing entity 10, a message receiver B acting through computing entity 20, and a trusted authority TA acting through computing entity 50 (this latter entity is not present in the prior art method and apparatus illustrated in Figure 1). The computing entities 10, 20 and 50 are typically based around program-controlled processors though some or all of the cryptographic functions may be implemented in dedicated hardware. The entities 10, 20 and 50 intercommunicate, for example, via the internet or other computer network though it is also possible that two or all three entities actually reside on the same computing platform. For convenience, the following description is given in terms of the parties A, B and TA, it being understood that these parties act through their respective computing entities. It is also to be understood that the message sent by the message sender to the message receiver can comprise any content and can, for example, simply be a symmetric cryptographic key.

[0015] As preferred embodiments of the invention are based on the ElGamal encryption/decryption scheme, this latter scheme will first be briefly reviewed with reference to Figure 1 in order to facilitate an understanding of the subsequently-described embodiments of the present invention. It is, however, to be understood that part of the contribution made by the inventors of the present invention is the appreciation of the possibilities offered by the ElGamal scheme in respect of IB cryptography as well as how these possibilities can be realised in practice.

Initial Set Up Phase

[0016]

1. B chooses random prime p .
2. B chooses a random number g in the range 2 to $(p-1)$.
3. B chooses a secret x .
4. B computes $y = g^x \bmod p$.
5. B publishes (g, p, y) and keeps x secret.

Message Transfer Phase

Message Encryption by Sender A

[0017]

6. A chooses a secret r .
7. A computes $h = g^r \bmod p$
8. A computes $J = (y^r) * m \bmod p$ where m is the message to be encrypted
9. A sends (h, J) to B.

Message Decryption by Recipient B

[0018]

10. B computes $J / h^x \bmod p$ to recover the message m .

[0019] As will be appreciated by persons skilled in the art, the sender A and recipient B can be considered as having effected a Diffie-Hellman type key exchange in that the quantity $y^r \bmod p$ computed by the sender A is equivalent to the quantity $h^x \bmod p$ computed by the recipient, (both these quantities corresponding to $g^{r \cdot x} \bmod p$, the Diffie-Hellman key distributed between A and B). However, it is also possible to consider the process in terms of B having a public key (g, p, y) and a private key x , the sender A using B's public key to encrypt the message m and B using its private key to recover the message.

[0020] Turning now to a consideration of embodiments of the present invention, in the Figure 2 embodiment the public/private keys belong to the trusted authority TA which is arranged to decrypt a message encrypted by the sender A. The encryption process effected by the sender A involves the use of a sender-chosen "identifier" string that comprises information concerning one or more actions (typically the checking of conditions indicated in the string) to be effected by the trusted authority before it decrypts the message, or before it releases the decrypted message to the recipient B. The string is provided to the trusted party and is a required component of the decryption process whereby any change in the string will result in a failure to correctly decrypt the message. The detailed steps of the Figure 2 method are set out below together with indications of typical bit sizes of the important quantities involved.

Initial Set Up Phase

[0021]

1. TA chooses random prime p (for example, 1024 bits).
2. TA chooses a random number g in the range 2 to $(p-1)$.
3. TA chooses a secret x (for example, a random, 160 bit, number).
4. TA computes $y = g^x \bmod p$.
5. TA publishes (g, p, y) and keeps x secret.

Message Transfer Phase

Message Encryption by Sender A

[0022]

6. A chooses an identifier string STR.
 7. A computes $z = \#(\text{STR})$ where $\#$ is a hash function (for example, SHA-1 returning 160 bits).
 8. A computes $y' = y^z \bmod p$
 9. A chooses a secret r (for example a random, 160 bit, number)
 10. A computes $h = g^r \bmod p$
 11. A computes $J = (y'^r) * m \bmod p$
 12. A sends (STR, h, J) to B and destroys r .
- (Steps 8 and 11 can be merged to have A compute J as: $(y^{z \cdot r}) * m \bmod p$)

Message Decryption for Recipient B by Trusted Authority TA

[0023]

- 5 13. B forwards (STR, h, J) to TA.
14. TA checks that B meets the conditions set out in STR.
15. TA computes $z = \#(\text{STR})$.
16. TA computes $J / h^{(z \cdot x)} \bmod p$ to recover the message m.
17. TA returns message m to B.
- 10 18. B receives recovered message m.

[0024] The transmissions are preferably integrity protected in any suitable manner.

[0025] With z and r both 160 bits, the main computational load on the sender is one 160-bit exponentiation and one 320-bit exponentiation (assuming steps 8 and 11 are combined), whilst the main computational load on the TA is one 320-bit exponentiation and one inversion.

[0026] It will be appreciated by persons skilled in the art that g should be chosen randomly but such that:

$$g^q = 1 \bmod p$$

where q is a large prime (typically at least 160 bits) that divides (p-1).

[0027] It should be noted that the multiplication effected in step 11 can be replaced by any modulo-p invertible operation for combining $y^{r \cdot z}$ and m (the operation being inverted in step 16). Thus, for example, J can be computed as:

$$m \oplus H(y^{r \cdot z} \bmod p)$$

where $\oplus$ is the Exclusive-OR function and H is a hash function. The message is subsequently recovered by the TA computing:

$$J \oplus H(h^{x \cdot z} \bmod p).$$

[0028] As regards the contents of the string STR chosen by the sender, as already indicated this string may be any string though in many cases restrictions will be placed on the string - for example, the string STR may be required to comply with a particular XML schema.

[0029] Generally, the string STR is used to convey to the trusted authority information concerning actions to be taken by the trusted authority when it receives the encrypted message for decryption. The information in the string STR may relate to actions to be taken by the trusted authority that do not affect message decryption - for example, the trusted authority TA may be required to send a message to the message sender A at the time the TA decrypts the message concerned. However, the information in the string STR will frequently specify one or more conditions to be checked by the trusted authority as being satisfied before the trusted authority decrypts the related encrypted message (or before returning the corresponding decrypted message to the recipient B concerned).

[0030] For example, the string STR may comprise a recipient identity condition identifying a specific intended message recipient; in this case, the trusted authority carries out an authentication process with the recipient B presenting the related message for decryption to check that the recipient concerned meets the recipient-identity condition.

[0031] Rather than identifying an intended recipient as a particular individual, the string STR may comprise one or more conditions specifying one or more non-identity attributes that the recipient must possess; for example, a condition may specify that a recipient must have a certain credit rating. Again, it is the responsibility of the trusted authority to check out this condition before producing the decrypted message for a recipient presenting the encrypted message for decryption.

[0032] The string STR may additionally or alternatively comprise one or more conditions unrelated to an attribute of the intended recipient; for example, a condition may be included that the message concerned is not to be decrypted before a particular date or time.

[0033] Whatever the conditions relate to, the string STR may directly set out the or each condition or may comprises

one or more condition identifiers specifying corresponding predetermined condition known to the trusted authority (in the latter case, the trusted authority uses the or each condition identifier to look up the corresponding condition to be checked).

[0034] In overview of the Figure 2 method, like the prior art method of Figure 1, it is possible to consider what is happening in terms of the Diffie-Hellman key distribution process. More particularly, the actions of the sender can be viewed as equivalent to:

deriving a Diffie-Hellman key ($g^{r \cdot x}$) from the key material y provided by the trusted party and the sender secret r ;
 exponentiating, modulo p , the Diffie-Hellman key using the string hash z as exponent,
 using the exponentiated key ($g^{r \cdot x \cdot z}$) to effect a modulo- p invertible operation involving the message m thereby to form an encrypted message.

Similarly, the actions of the TA can be viewed as equivalent to:

deriving the Diffie-Hellman key ($g^{r \cdot x}$) from the sender key material h and the TA's secret x ,
 exponentiating, modulo p , the Diffie-Hellman key using the string hash z as exponent,
 applying the exponentiated key ($g^{r \cdot x \cdot z}$) to the encrypted message to invert the sender-effected invertible operation thereby to recover the message.

[0035] Alternatively, viewed in terms of the TA having a public key (p, g, y) and private key (x), in the Figure 2 process the sender A effectively modifies the TA public key using the hash of the string STR as an exponent for exponentiation, modulo p , of the element y of that key. The sender A also supplies the string to the TA to enable it to effect a complimentary modification to its private key by multiplying the private key x by the hash of the string. Where the string comprises information serving to identify an intended recipient B of the message m , the modification of the TA's public key can be thought of as a customization of the public key to the intended recipient B. This process of modifying another party's public key by using the hash of a string STR as an exponent for exponentiation of at least an element of the public key, is not restricted to the ElGamal-based encryption/decryption described above and can be effected in connection with any suitable cryptographic process.

[0036] A potential drawback of the Figure 2 embodiment is that the TA can read the messages m . In order to prevent this, B can blind the encrypted message before sending it to TA for decryption, B subsequently un-blinding the decrypted, but still blinded, message returned by the TA to recover the message m . By way of example, step 13 of Figure 2 can be replaced by:

13a B chooses a blinding secret k (for example, 1024 bits).
 13b. B computes $J' = J \cdot k \bmod p$
 13c. B sends (STR, h, J') to TA

[0037] The TA carries out its processing steps 14 to 18 as before but using J' rather than J ; the result of step 16 is now the recovery of mk - that is, the blinded but decrypted message - rather than the message m . In order for B to un-blind the message, step 18 now becomes:

18a. B receives the blinded, decrypted message mk .
 18b. B computes $(mk / k) \bmod p$ to recover the message m ; thereafter, B destroys k .

The full process including the above blinding is shown in Figure 3.

[0038] It will be appreciated that the blinding / un-blinding operations can differ from those described above. For example, blinding can be effected by computing a modulo- p division of J by k , in which case un-blinding would be effected by a modulo- p multiplication by k of the decrypted, but still blinded, message returned by the TA.

[0039] Many variants are possible to the above-described embodiments of the invention. Thus, in certain situations it may be required that a message should only be decryptable with the cooperation of multiple trusted authorities each of which would typically have a different associated public and private data. One such situation where this may be desirable is where the sender wishes to impose multiple conditions but no single trusted authority is competent to check all conditions - in this case, different trusted authorities can be used to check different conditions. Another situation in which multiple trusted authorities may be required is where there is a concern that a trust authority may have access to the encrypted, but not blinded, messages passing from A to B and it is important to prevent the trust authority reading the messages - in this case, multiple trusted authorities can be used together in a manner such that no one authority can read the messages passing from A to B.

[0040] Various arrangements are possible for involving multiple trusted authorities, including:

- the sender organizes the message content as a number of data sets (say k data sets) by using Shamir's secret sharing scheme and then encrypts each data set using an associated string STR (for example, specifying a respective condition to be checked) and the public modulus of a respective one of the trusted authorities; in order to retrieve the message, a recipient B has to go to all of the trusted authorities in order to decrypt all of the data sets because any k-1 data sets or less cannot disclose any of the message contents.
- the sender can use the encrypted data resulting from encrypting message data using a first string (for example, specifying a particular condition) and the public modulus of a first trusted authority as the data to be encrypted using a second string and the public modulus of a second trusted authority and so on; the encrypted data resulting from the encryption effected in respect of all trusted authorities to be used then being sent to the recipient B for decryption in successive decryption operations by the corresponding trusted authorities.

Claims

1. A cryptographic method in which a sender (A) encrypts and sends a message to a recipient (B) for decryption by a trusted party (TA), the sender (A) being in possession of a public key for which there exists a corresponding private key held by the trusted party (TA), the method comprising:

the sender (A) modifying the public key by exponentiating at least one element of that key using as exponent a hash of a string (STR) that comprises information concerning at least one action to be taken by the trusted party (TA), and using the modified public key to encrypt said message;
the recipient (B) receiving the encrypted message and said string (STR) and passing them to the trusted party; and
the trusted party (TA) using said string (STR) to modify its private key to compliment the modified public key, decrypting the message with the modified private key, and returning the decrypted message to the recipient (B) after carrying out said at least one action with a satisfactory conclusion..

2. A method according to claim 1, wherein:

the received public key comprises elements p, g and y, the element y corresponding to $g^x \bmod p$, where x is a private key belonging to the trusted party (TA); and
the sender (A) modifies the public key by effecting a modulo-p exponentiation of the element y using the hash of said string (STR) as exponent.

3. A method according to claim 2, wherein the trusted party (TA) modifies its private key, in relation to use in connection with the modified public key, by an operation equivalent to multiplying its private key by the hash of the string (STR).

4. A method according to claim 2, wherein:

the sender (A) uses the modified public key to encrypt the message m by effecting a modulo-p exponentiation of the modified public key element using a secret r as exponent, and then combining the result and the message m using a modulo-p invertible operation to form a value J;
the sender (A) sends to the recipient (B), in addition to said string, the value J and a value h corresponding to $g^r \bmod p$.

5. A method according to claim 4, wherein the public-key related exponentiations effected by the sender (A) are effected together as a single exponentiation operation.

6. A method according to claim 4, wherein said invertible operation comprises multiplying the message by the said result of exponentiation of the modified public key element using the secret r.

7. A method according to claim 6, wherein the trusted party (TA) decrypts the encrypted message by computing a value z as the hash of said string (STR) and then computing:

$$J/h^{z.x} \bmod p;$$

the trusted party (TA) only decrypting the message, or only releasing the decrypted message, after carrying out said at least one action with a satisfactory conclusion.

8. A method according to claim 7, wherein:

the recipient (B), prior to forwarding the value J to the trusted party (TA) for decryption, subjects it to a modulo-p blinding operation using a factor k where k is a secret random number; and the trusted party (TA) provides the decrypted, but still blinded message, back to the recipient (B) provided said at least one action has been carried out with a satisfactory conclusion, the recipient (B) thereupon canceling the blinding to recover the message.

9. A method according to claim 4, wherein said invertible operation comprises effecting an exclusive OR combination of the message with a hash of the said result of exponentiation of the modified public key element using the secret r.

10. A method according to claim 9, wherein the trusted party (TA) decrypts the encrypted message by computing a value z as the hash of said string (STR) and then computing:

$$J \oplus H(h^{z.x} \bmod p)$$

where $\oplus$ is the Exclusive-OR function and H is a hash function; the trusted party (TA) only decrypting the message, or only releasing the decrypted message, after carrying out said at least one action with a satisfactory conclusion.

11. A method according to claim 10, wherein:

the recipient (B) prior to forwarding the value J to the trusted party (TA) for decryption, subjects it to a modulo-p blinding operation using a factor k where k is a secret random number; and the trusted party (TA) provides the decrypted, but still blinded message, back to the recipient (B) provided said at least one action has been carried out with a satisfactory conclusion, the recipient (B) thereupon canceling the blinding to recover the message.

12. A method according to claim 1, wherein said at least one action comprises a check that a condition has been met.

13. A method according to claim 1, wherein said at least one action comprises a check relating to the identity of the recipient.

14. A cryptographic method, wherein a trusted party (TA) with secret x and public parameters p and g, effects at least steps of:

receiving values h and J and a condition string STR from a message sender (A), the condition string comprising at least one condition to be checked by the trusted party (TA); computing:

$$z \#(\text{STR}), \text{ where } \# \text{ is a hash function;}$$

computing:

$$f^1(J, h^{z.x})$$

where $f^1()$ inverts an invertible operation $f()$, whereby to produce a result which corresponds to a decrypted message m when:

the received value of h corresponds to $g^r \bmod p$ where r is a secret belonging to the sender (A), and the received value of J corresponds to $f(g^{r.x.z}, m)$;

the trusted party (TA) only computing said result, or only releasing the result, after confirming that said at least one

condition contained in the string has been met.

15. A method according to claim 14, wherein $f^1()$ corresponds to computing:

$$J/h^{z \cdot x} \bmod p$$

the result being the message m when the received value of J is: $(g^{r \cdot x \cdot z}) * m \bmod p$.

16. A method according to claim 14, wherein $f^1()$ corresponds to computing:

$$J \oplus H(h^{z \cdot x} \bmod p)$$

where H is a predetermined hash function, the result being the message m when the received value of J is: $m \oplus H(g^{r \cdot x \cdot z}) \bmod p$

17. A method according to claim 14, wherein the received value of J is a blinded value whereby said result is a blinded result.

18. Cryptographic apparatus comprising first, second and third computing entities, the first computing entity (A) comprising:

an input arrangement for receiving a public key for which there exists a corresponding private key held by the second computing entity (TA),
a key-processing arrangement arranged to modify the public key by exponentiating at least one element of the received public key using as exponent a hash of a string (STR), this string comprising information concerning at least one action to be taken by the second computing entity (TA),
an encryption arrangement for encrypting a message using the modified public key; and
an output arrangement for outputting the encrypted message and said string;

the third computing entity (B) being arranged to receive the encrypted message and the string and pass them to the second computing entity (TA), and the second computing entity (TA) being arranged to receive message and the string, to use the string to modify its private key to compliment the modified public key, and to decrypt the message using the modified private key, the second computing entity (TA) being arranged to only decrypt the message, or only release the decrypted message, after carrying out said at least one action with a satisfactory conclusion.

19. Apparatus according to claim 18, wherein the received public key comprises elements p , g and y , the element y corresponding to $g^x \bmod p$, where x is a private key belonging to the second computing entity (TA) the key-processing arrangement of the first computing entity (A) being arranged to modify the received public key by effecting a modulo- p exponentiation of the element y using the hash of said string (STR) as exponent.

20. Apparatus according to claim 19, wherein the second computing entity (TA) is arranged to modify its private key, in relation to use in connection with the modified public key, by an operation equivalent to multiplying its private key by the hash of the string (STR).

21. Apparatus according to claim 19, wherein the encryption arrangement of the first computing entity (A) is arranged to encrypt the message m by effecting a modulo- p exponentiation of the modified public key element using a secret r as exponent, and then combining the result and the message m using a modulo- p invertible operation to form a value J ; the output arrangement of the first computing entity (A) being arranged to output the value J and a value h corresponding to $g^r \bmod p$.

22. Apparatus according to claim 21, wherein the key-processing arrangement and encryption arrangement of the first computing entity (A) are integrated and arranged such that the public-key related exponentiations effected by these two arrangements are effected together as a single exponentiation operation.

23. Apparatus according to claim 21, wherein the encryption arrangement is arranged to carry out said invertible operation

by multiplying the message by the said result of exponentiation of the modified public key element using the secret r .

24. Apparatus according to claim 23, wherein the second computing entity (TA) is arranged to decrypt the encrypted message by computing a value z as the hash of said string (STR) and then computing:

$$J/h^{z \cdot x} \bmod p;$$

25. Apparatus according to claim 24, wherein the third computing entity (B) arranged to receive the value J and to subject it to a modulo- p blinding operation using a factor k where k is a secret random number, before forwarding the blinded value J to the second computing entity (TA); the second computing entity being arranged to carry out message decryption and return the decrypted, but still blinded message, back to the third computing entity (B) provided said at least one action has been carried out with a satisfactory conclusion; and the third computing entity (B) being further arranged to receive the decrypted, but still blinded, message and to cancel the blinding to recover the message.

26. Apparatus according to claim 21, wherein the encryption arrangement is arranged to carry out said invertible operation by effecting an exclusive OR combination of the message with a hash of the said result of exponentiation of the modified public key element using the secret r .

27. Apparatus according to claim 26, wherein the second computing entity (TA) is arranged to decrypt the encrypted message by computing a value z as the hash of said string (STR) and then computing:

$$J \oplus H(h^{z \cdot x} \bmod p)$$

where $\oplus$ is the Exclusive-OR function and H is a hash function;

28. Apparatus according to claim 27, wherein the third computing entity (B) is arranged to receive the value J and to subject it to a modulo- p blinding operation using a factor k where k is a secret random number, before forwarding the blinded value J to the second computing entity (TA); the second computing entity being arranged to carry out message decryption and return the decrypted, but still blinded message, back to the third computing entity (B) provided said at least one action has been carried out with a satisfactory conclusion; and the third computing entity being (B) further arranged to receive the decrypted, but still blinded, message and to cancel the blinding to recover the message.

29. A trusted-party entity (TA) comprising:

a data store for storing a secret x and public parameters p and g ;

an input arrangement for receiving values h and J and a condition string STR from a message sender (A), the condition string comprising at least one condition to be checked by the trusted party;
a processing arrangement arranged to compute:

$$z \leftarrow \#(\text{STR}) \text{ where } \# \text{ is a hash function; and } f^1(J, h^{z \cdot x})$$

where $f^1()$ inverts an invertible operation $f()$, whereby to produce a result which corresponds to a decrypted message m when:

the received value of h corresponds to $g^r \bmod p$ where r is a secret belonging to the sender, and
the received value of J corresponds to $f(g^{r \cdot x \cdot z}, m)$;

an output arrangement for outputting said result; and
a control arrangement arranged to check that said at least one condition contained in the string STR has been met, and only permit the processing arrangement to compute said result, or only permit said output arrangement to output said result,

where said at least one condition has been met.

30. A trusted-party entity (TA) according to claim 29, wherein $f^1()$ corresponds to computing:

$$J/h^{z \cdot x} \bmod p$$

the result being the message m when the received value of J is: $(g^{r \cdot x \cdot z}) * m \bmod p$.

31. A trusted-party entity (TA) according to claim 29, wherein $f^1()$ corresponds to computing:

$$J \oplus H(h^{z \cdot x} \bmod p)$$

where H is a predetermined hash function, the result being the message m when the received value of J is: $m \oplus H(g^{r \cdot x \cdot z} \bmod p)$

32. A trusted-party entity (TA) according to claim 29, wherein the received value of J is a blinded value whereby said result is a blinded result.

Patentansprüche

1. Ein kryptographisches Verfahren, bei dem ein Absender (A) eine Nachricht verschlüsselt und an einen Empfänger (B) sendet, zur Entschlüsselung durch einen vertrauenswürdigen Teilnehmer (TA), wobei der Absender (A) in Besitz eines öffentlichen Schlüssels ist, für den es einen entsprechenden privaten Schlüssel gibt, der durch den vertrauenswürdigen Teilnehmer (TA) gehalten wird, wobei das Verfahren folgende Schritte aufweist:

Modifizieren, durch den Absender (A), des öffentlichen Schlüssels durch Potenzieren zumindest eines Elements dieses Schlüssels unter Verwendung eines Hash einer Zeichenfolge (STR) als Exponent, die Informationen bezüglich zumindest einer Aktion aufweist, die durch den vertrauenswürdigen Teilnehmer (TA) durchgeführt werden soll, und unter Verwendung des modifizierten öffentlichen Schlüssels zur Verschlüsselung der Nachricht; Empfangen, durch den Empfänger (B), der verschlüsselten Nachricht und der Zeichenfolge (STR) und Weiterleiten derselben an den vertrauenswürdigen Teilnehmer; und Verwenden, durch den vertrauenswürdigen Teilnehmer (TA), der Zeichenfolge (STR) zum Modifizieren seines privaten Schlüssels zum Ergänzen des modifizierten öffentlichen Schlüssels, Entschlüsseln der Nachricht mit dem modifizierten privaten Schlüssel und Zurückgeben der entschlüsselten Nachricht an den Empfänger (B) nach einer Ausführung der zumindest einen Aktion mit einem zufriedenstellenden Abschluss.

2. Ein Verfahren gemäß Anspruch 1, bei dem:

der empfangene öffentliche Schlüssel Elemente p , g und y aufweist, wobei das Element y $g^x \bmod p$ entspricht, wobei x ein privater Schlüssel ist, der zu dem vertrauenswürdigen Teilnehmer (TA) gehört; und der Absender (A) den öffentlichen Schlüssel durch Ausführen einer Modulo- p -Potenzierung des Elements y unter Verwendung des Hash der Zeichenfolge (STR) als Exponent modifiziert.

3. Ein Verfahren gemäß Anspruch 2, bei dem der vertrauenswürdige Teilnehmer (TA) seinen privaten Schlüssel in Bezug auf eine Verwendung in Verbindung mit dem modifizierten öffentlichen Schlüssel durch eine Operation modifiziert, die äquivalent zu einem Multiplizieren seines privaten Schlüssels mit dem Hash der Zeichenfolge (STR) ist.

4. Ein Verfahren gemäß Anspruch 2, bei dem:

der Absender (A) den modifizierten öffentlichen Schlüssel verwendet, um die Nachricht m zu verschlüsseln, indem eine Modulo- p -Potenzierung des Elements des modifizierten öffentlichen Schlüssels unter Verwendung eines geheimen r als Exponent ausgeführt wird und dann das Ergebnis und die Nachricht m unter Verwendung

einer invertierbaren Modulo-p-Operation kombiniert werden, um einen Wert J zu bilden;
der Absender (A) den Wert J und einen Wert h entsprechend $g^r \bmod p$ zusätzlich zu der Zeichenfolge an den Empfänger (B) sendet.

- 5 5. Ein Verfahren gemäß Anspruch 4, bei dem die Potenzierungen mit Bezug auf den öffentlichen Schlüssel, die durch den Absender (A) ausgeführt werden, gemeinsam als eine einzelne Potenzierungsoperation ausgeführt werden.
6. Ein Verfahren gemäß Anspruch 4, bei dem die invertierbare Operation ein Multiplizieren der Nachricht mit dem Ergebnis einer Potenzierung des Elements des modifizierten öffentlichen Schlüssels unter Verwendung des geheimen r aufweist.
- 10 7. Ein Verfahren gemäß Anspruch 6, bei dem der vertrauenswürdige Teilnehmer (TA) die verschlüsselte Nachricht durch ein Berechnen eines Werts z als Hash der Zeichenfolge (STR) und darauffolgendes Berechnen von:

$$J/h^{z,x} \bmod p$$

entschlüsselt; wobei der vertrauenswürdige Teilnehmer (TA) die Nachricht nur entschlüsselt oder die entschlüsselte Nachricht nur freigibt, nachdem die zumindest eine Aktion mit einem zufriedenstellenden Abschluss ausgeführt wurde.

8. Ein Verfahren gemäß Anspruch 7, bei dem:

der Empfänger (B) vor einem Weiterleiten des Werts J an den vertrauenswürdigen Teilnehmer (TA) zur Entschlüsselung denselben einer Modulo-p-Verdeckungsoperation unter Verwendung eines Faktors k unterzieht, wobei k eine geheime Zufallszahl ist; und
der vertrauenswürdige Teilnehmer (TA) die entschlüsselte, jedoch noch verdeckte Nachricht zurück an den Empfänger (B) liefert, unter der Voraussetzung, dass die zumindest eine Aktion mit einem zufriedenstellenden Abschluss ausgeführt wurde, wobei der Empfänger (B) daraufhin die Verdeckung aufhebt, um die Nachricht wiederzugewinnen.

9. Ein Verfahren gemäß Anspruch 4, bei dem die invertierbare Operation ein Ausführen einer Exklusiv-ODER-Kombination der Nachricht mit einem Hash des Ergebnisses einer Potenzierung des Elements des modifizierten öffentlichen Schlüssels unter Verwendung des geheimen r aufweist.
10. Ein Verfahren gemäß Anspruch 9, bei dem der vertrauenswürdige Teilnehmer (TA) die verschlüsselte Nachricht durch ein Berechnen eines Werts z als Hash der Zeichenfolge (STR) und ein darauffolgendes Berechnen von:

$$J \oplus H(h^{z,x} \bmod p)$$

entschlüsselt, wobei $\oplus$ die Exklusiv-ODER-Funktion ist und H eine Hash-Funktion ist;
wobei der vertrauenswürdige Teilnehmer (TA) die Nachricht nur entschlüsselt oder die entschlüsselte Nachricht nur freigibt, nachdem die zumindest eine Aktion mit einem zufriedenstellenden Abschluss ausgeführt wurde.

11. Ein Verfahren gemäß Anspruch 10, bei dem:

der Empfänger (B) vor dem Weiterleiten des Werts J an den vertrauenswürdigen Teilnehmer (TA) zur Entschlüsselung denselben einer Modulo-p-Verdeckungsoperation unter Verwendung eines Faktors k unterzieht, wobei k eine geheime Zufallszahl ist; und
der vertrauenswürdige Teilnehmer (TA) die entschlüsselte, jedoch noch verdeckte Nachricht zurück an den Empfänger (B) liefert, unter der Voraussetzung, dass die zumindest eine Aktion mit einem zufriedenstellenden Abschluss ausgeführt wurde, wobei der Empfänger (B) daraufhin die Verdeckung aufhebt, um die Nachricht wiederzugewinnen.

12. Ein Verfahren gemäß Anspruch 1, bei dem die zumindest eine Aktion eine Prüfung, dass eine Bedingung erfüllt

wurde, aufweist.

13. Ein Verfahren gemäß Anspruch 1, bei dem die zumindest eine Aktion eine Prüfung in Bezug auf die Identität des Empfängers aufweist.

14. Ein kryptographisches Verfahren, bei dem ein vertrauenswürdiger Teilnehmer (TA) mit geheimem x und öffentlichen Parametern p und g zumindest folgende Schritte ausführt:

Empfangen von Werten h und J und einer Bedingungszeichenfolge STR von einem Nachrichtenabsender (A), wobei die Bedingungszeichenfolge zumindest eine Bedingung aufweist, die durch den vertrauenswürdigen Teilnehmer (TA) geprüft werden soll;
Berechnen von:

$z \leftarrow \#(\text{STR})$, wobei $\#$ eine Hash-Funktion ist;

Berechnen von:

$$f^{-1}(J, h^{z,x})$$

wobei $f^{-1}()$ eine invertierbare Operation $f()$ invertiert, um dadurch ein Ergebnis zu erzeugen, das einer entschlüsselten Nachricht m entspricht, wenn:

der empfangene Wert von $h g^r \bmod p$ entspricht, wobei r ein Geheimnis ist, das zu dem Absender (A) gehört, und
der empfangene Wert von $J f(g^{r,x,z}, m)$ entspricht;

wobei der vertrauenswürdige Teilnehmer (TA) das Ergebnis nur berechnet oder das Ergebnis nur freigibt, nachdem bestätigt wurde, dass die zumindest eine Bedingung, die in der Zeichenfolge beinhaltet ist, erfüllt wurde.

15. Ein Verfahren gemäß Anspruch 14, bei dem $f^{-1}()$ einem Berechnen von:

$$J/h^{z,x} \bmod p$$

entspricht, wobei das Ergebnis die Nachricht m ist, wenn der empfangene Wert von $J (g^{r,x,z}) \cdot m \bmod p$ ist.

16. Ein Verfahren gemäß Anspruch 14, bei dem $f^{-1}()$ einem Berechnen von:

$$J \oplus H(h^{z,x} \bmod p)$$

entspricht, wobei H eine vorbestimmte Hash-Funktion ist, wobei das Ergebnis die Nachricht m ist, wenn der empfangene Wert von $J m \oplus H(g^{r,x,z}) \bmod p$ ist.

17. Ein Verfahren gemäß Anspruch 14, bei dem der empfangene Wert von J ein verdeckter Wert ist, wodurch das Ergebnis ein verdecktes Ergebnis ist.

18. Kryptographische Vorrichtung, die eine erste, zweite und dritte Rechenentität aufweist, wobei die erste Rechenentität (A) folgende Merkmale aufweist:

eine Eingangsanordnung zum Empfangen eines öffentlichen Schlüssels, für den es einen entsprechenden privaten Schlüssel gibt, der durch die zweite Rechenentität (TA) gehalten wird,
eine Schlüsselverarbeitungsanordnung, die angeordnet ist, um den öffentlichen Schlüssel zu modifizieren, indem zumindest ein Element des empfangenen öffentlichen Schlüssels unter Verwendung eines Hash einer

Zeichenfolge (STR) als Exponent potenziert wird, wobei diese Zeichenfolge Informationen bezüglich zumindest einer Aktion, die durch die zweite Rechenentität (TA) durchgeführt werden soll, aufweist, eine Entschlüsselungsanordnung zum Entschlüsseln einer Nachricht unter Verwendung des modifizierten öffentlichen Schlüssels; und

eine Ausgangsanordnung zum Ausgeben einer Nachricht unter Verwendung des modifizierten öffentlichen Schlüssels;

wobei die dritte Rechenentität (B) angeordnet ist, um die verschlüsselte Nachricht und die Zeichenfolge zu empfangen und dieselben an die zweite Rechenentität (TA) weiterzuleiten, und die zweite Rechenentität (TA) angeordnet ist, um die Nachricht und die Zeichenfolge zu empfangen, um die Zeichenfolge zu verwenden, um ihren privaten Schlüssel zu modifizieren, um den modifizierten privaten Schlüssel zu ergänzen, und um die Nachricht unter Verwendung des modifizierten privaten Schlüssels zu entschlüsseln, wobei die zweite Rechenentität (TA) angeordnet ist, um die Nachricht nur zu entschlüsseln oder die entschlüsselte Nachricht nur freizugeben, nachdem die zumindest eine Aktion mit einem zufriedenstellenden Abschluss ausgeführt wurde.

19. Vorrichtung gemäß Anspruch 18, bei der der empfangene öffentliche Schlüssel Elemente p , g und y aufweist, wobei das Element $y = g^x \bmod p$ entspricht, wobei x ein privater Schlüssel ist, der zu der zweiten Rechenentität (TA) gehört, wobei die Schlüsselverarbeitungsanordnung der ersten Rechenentität (A) angeordnet ist, um den empfangenen öffentlichen Schlüssel zu modifizieren, indem eine Modulo- p -Potenzierung des Elements y unter Verwendung des Hash der Zeichenfolge (STR) als Exponent ausgeführt wird.

20. Vorrichtung gemäß Anspruch 19, bei der die zweite Rechenentität (TA) angeordnet ist, um ihren privaten Schlüssel in Bezug auf eine Verwendung in Verbindung mit dem modifizierten öffentlichen Schlüssel durch eine Operation zu modifizieren, die äquivalent zu einem Multiplizieren ihres privaten Schlüssels mit dem Hash der Zeichenfolge (STR) ist.

21. Vorrichtung gemäß Anspruch 19, bei der die Verschlüsselungsanordnung der ersten Rechenentität (A) angeordnet ist, um die Nachricht m zu verschlüsseln, indem eine Modulo- p -Potenzierung des Elements des modifizierten öffentlichen Schlüssels unter Verwendung eines geheimen r als Exponent ausgeführt wird und dann das Ergebnis und die Nachricht m unter Verwendung einer invertierbaren Modulo- p -Operation kombiniert werden, um einen Wert J zu bilden; wobei die Ausgangsanordnung der ersten Rechenentität (A) angeordnet ist, um den Wert J und einen Wert h , der $g^r \bmod p$ entspricht, auszugeben.

22. Vorrichtung gemäß Anspruch 21, bei der die Schlüsselverarbeitungsanordnung und die Verschlüsselungsanordnung der ersten Rechenentität (A) derart integriert und angeordnet sind, dass die Potenzierungen in Bezug auf den öffentlichen Schlüssel, die durch diese beiden Anordnungen ausgeführt werden, gemeinsam als eine einzelne Potenzierungsoperation ausgeführt werden.

23. Vorrichtung gemäß Anspruch 21, bei der die Verschlüsselungsanordnung angeordnet ist, um die invertierbare Operation auszuführen, indem die Nachricht mit dem Ergebnis einer Potenzierung des Elements des modifizierten öffentlichen Schlüssels unter Verwendung eines geheimen r multipliziert wird.

24. Vorrichtung gemäß Anspruch 23, bei der die zweite Rechenentität angeordnet ist, um die verschlüsselte Nachricht zu entschlüsseln, indem ein Wert z als Hash der Zeichenfolge (STR) berechnet wird und indem dann:

$$J/h^{z,x} \bmod p$$

berechnet wird.

25. Vorrichtung gemäß Anspruch 24, bei der die dritte Rechenentität (B) angeordnet ist, um den Wert J zu empfangen und denselben einer Modulo- p -Verdeckungsoperation unter Verwendung eines Faktors k zu unterziehen, wobei k eine geheime Zufallszahl ist, bevor der verdeckte Wert J an die zweite Rechenentität (TA) weitergeleitet wird; wobei die zweite Rechenentität angeordnet ist, um eine Nachrichtenentschlüsselung auszuführen und die entschlüsselte, jedoch noch verdeckte Nachricht an die dritte Rechenentität (B) zurückzugeben, unter der Voraussetzung, dass die zumindest eine Aktion mit einem zufriedenstellenden Abschluss ausgeführt wurde; und wobei die dritte Rechenentität (B) ferner angeordnet ist, um die entschlüsselte, jedoch noch verdeckte Nachricht zu empfangen und die Verdeckung aufzuheben, um die Nachricht wiederzugewinnen.

26. Vorrichtung gemäß Anspruch 21, bei der die Verschlüsselungsanordnung angeordnet ist, um die invertierbare Operation auszuführen, indem eine Exklusiv-ODER-Kombination der Nachricht mit einem Hash des Ergebnisses einer Potenzierung des Elements des modifizierten öffentlichen Schlüssels unter Verwendung des geheimen r ausgeführt wird.

27. Vorrichtung gemäß Anspruch 26, bei der die zweite Rechenentität (TA) angeordnet ist, um die verschlüsselte Nachricht durch ein Berechnen eines Werts z als Hash der Zeichenfolge (STR) und ein darauffolgendes Berechnen von:

$$J \oplus H(h^{z,x} \bmod p)$$

zu entschlüsseln, wobei $\oplus$ die Exklusiv-ODER-Funktion ist und H eine Hash-Funktion ist.

28. Vorrichtung gemäß Anspruch 27, bei der die dritte Rechenentität (B) angeordnet ist, um den Wert J zu empfangen und denselben einer Modulo- p -Verdeckungsoperation unter Verwendung eines Faktors k zu unterziehen, wobei k eine geheime Zufallszahl ist, bevor der verdeckte Wert J an die zweite Rechenentität (TA) weitergeleitet wird; wobei die zweite Rechenentität angeordnet ist, um eine Nachrichtenentschlüsselung auszuführen und die entschlüsselte, jedoch noch verdeckte Nachricht an die dritte Rechenentität (B) zurückzugeben, unter der Voraussetzung, dass die zumindest eine Aktion mit einem zufriedenstellenden Abschluss ausgeführt wurde; und die dritte Rechenentität (B) ferner angeordnet ist, um die entschlüsselte, jedoch noch verdeckte Nachricht zu empfangen und die Verdeckung aufzuheben, um die Nachricht wiederzugewinnen.

29. Eine Vertrauenswürdig-Teilnehmer-Entität (TA), die folgende Merkmale aufweist:

einen Datenspeicher zum Speichern eines geheimen x und öffentlicher Parameter p und g ;
eine Eingangsanordnung zum Empfangen von Werten h und J und einer Bedingungszeichenfolge STR von einem Nachrichtenabsender (A), wobei die Bedingungszeichenfolge zumindest eine Bedingung aufweist, die durch den vertrauenswürdigen Teilnehmer überprüft werden soll;
eine Verarbeitungsanordnung, die angeordnet ist, um Folgendes zu berechnen:

$$z \leftarrow \#(\text{STR}), \text{ wobei } \# \text{ eine Hash-Funktion ist; und} \\ f^{-1}(J, h^{z,x})$$

wobei $f^{-1}()$ eine invertierbare Operation $f()$ invertiert, um dadurch ein Ergebnis zu erzeugen, das einer entschlüsselten Nachricht m entspricht, wenn:

der empfangene Wert von $h g^r \bmod p$ entspricht, wobei r ein Geheimnis ist, das zu dem Absender gehört, und der empfangene Wert von $J f(g^{r,x,z}, m)$ entspricht;

eine Ausgangsanordnung zum Ausgeben des Ergebnisses; und
eine Steueranordnung, die angeordnet ist, um zu prüfen, dass die zumindest eine Bedingung, die in der Zeichenfolge STR beinhaltet ist, erfüllt wurde, und nur zu erlauben, dass die Verarbeitungsanordnung das Ergebnis berechnet, oder nur zu erlauben, dass die Ausgangsanordnung das Ergebnis ausgibt, wenn die zumindest eine Bedingung erfüllt wurde.

30. Eine Vertrauenswürdig-Teilnehmer-Entität (TA) gemäß Anspruch 29, bei der $f^{-1}()$ einem Berechnen von:

$$J/h^{z,x} \bmod p$$

entspricht, wobei das Ergebnis die Nachricht m ist, wenn der empfangene Wert von $J (g^{r,x,z}) \cdot m \bmod p$ ist.

31. Eine Vertrauenswürdig-Teilnehmer-Entität (TA) gemäß Anspruch 29, bei der $f^{-1}()$ einem Berechnen von:

$$J \oplus H(h^{z,x} \bmod p)$$

5
entspricht, wobei H eine vorbestimmte Hash-Funktion ist, wobei das Ergebnis die Nachricht m ist, wenn der empfangene Wert von $J \oplus H(g^{r,x,z} \bmod p)$ ist.

10
32. Eine Vertrauenswürdiger-Teilnehmer-Entität (TA) gemäß Anspruch 29, bei der der empfangene Wert von J ein verdeckter Wert ist, wodurch das Ergebnis ein verdecktes Ergebnis ist.

Revendications

15
1. Procédé cryptographique dans lequel un expéditeur (A) chiffre et envoie un message à un destinataire (B) pour un déchiffrement par une partie de confiance (TA), l'expéditeur (A) étant en possession d'une clé publique pour laquelle il existe une clé privée correspondante détenue par la partie de confiance (TA), le procédé comprenant les étapes consistant à :

20
■ pour l'expéditeur (A), modifier la clé publique en élevant à une puissance au moins un élément de cette clé au moyen d'un exposant d'un adressage calculé d'une chaîne (STR) qui comprend des informations concernant au moins une action qui doit être entreprise par la partie de confiance (TA), et au moyen de la clé publique modifiée pour chiffrer ledit message ;

25
■ pour le destinataire (B), recevoir le message chiffré et ladite chaîne (STR) et les transmettre à la partie de confiance ; et

■ pour la partie de confiance (TA), utiliser ladite chaîne (STR) pour modifier sa clé privée afin de compléter la clé publique modifiée, déchiffrer le message avec la clé privée modifiée, et retourner le message déchiffré au destinataire (B) après exécution de ladite au moins une action avec une conclusion satisfaisante.

30
2. Procédé selon la revendication 1, dans lequel:

■ la clé publique reçue comprend des éléments p, g et y, l'élément y correspondant à $g^x \bmod p$, où x est une clé privée appartenant à la partie de confiance (TA) ; et

35
■ l'expéditeur (A) modifie la clé publique en effectuant une élévation à une puissance modulo-p de l'élément y au moyen de l'adressage calculé de ladite chaîne (STR) en tant qu'exposant.

40
3. Procédé selon la revendication 2, dans lequel la partie de confiance (TA) modifie sa clé privée, par rapport à une utilisation en liaison avec la clé publique modifiée, par une opération équivalente à une multiplication de sa clé privée par l'adressage calculé de la chaîne (STR).

45
4. Procédé selon la revendication 2, dans lequel:

■ l'expéditeur (A) utilise la clé publique modifiée pour chiffrer le message m en effectuant une élévation à une puissance modulo-p de l'élément de clé publique modifiée au moyen d'une valeur secrète r en tant qu'exposant, puis en combinant le résultat et le message m au moyen d'une opération réversible modulo-p pour former une valeur J ;

■ l'expéditeur (A) envoie au destinataire (B), en plus de ladite chaîne, la valeur J et une valeur h correspondant à $g^r \bmod p$.

50
5. Procédé selon la revendication 4, dans lequel les élévations à une puissance concernant une clé publique effectuées par l'expéditeur (A) sont effectuées ensemble comme une seule opération d'élévation à une puissance.

55
6. Procédé selon la revendication 4, dans lequel ladite opération réversible comprend l'étape consistant à multiplier le message par ledit résultat de l'élévation à une puissance de l'élément de clé publique modifiée au moyen de la valeur secrète r.

7. Procédé selon la revendication 6, dans lequel la partie de confiance (TA) déchiffre le message chiffré en calculant une valeur z en tant qu'adressage calculé de ladite chaîne (STR) puis en calculant:

$$J/h^{z \cdot x} \bmod p ;$$

5 la partie de confiance (TA) déchiffrant uniquement le message, ou émettant uniquement le message déchiffré, après exécution de ladite au moins une action avec une conclusion satisfaisante.

8. Procédé selon la revendication 7, dans lequel:

10 ■ le destinataire (B), avant de transférer la valeur J à la partie de confiance (TA) pour déchiffrement, la soumet à une opération de dissimulation modulo-p au moyen d'un facteur k où k est un nombre aléatoire secret ; et
 ■ la partie de confiance (TA) renvoie le message déchiffré, mais toujours dissimulé, au destinataire (B) à condition que ladite au moins une action ait été exécutée avec une conclusion satisfaisante, le destinataire (B) annulant sur ce la dissimulation pour récupérer le message.

15 9. Procédé selon la revendication 4, dans lequel ladite opération réversible comprend l'étape consistant à effectuer une combinaison OU exclusive du message avec un adressage calculé dudit résultat de l'élévation à une puissance de l'élément de clé publique modifiée au moyen de la valeur secrète r.

20 10. Procédé selon la revendication 9, dans lequel la partie de confiance (TA) déchiffre le message chiffré en calculant une valeur z en tant qu'adressage calculé de ladite chaîne (STR) et en calculant:

$$J \oplus H(h^{z \cdot x} \bmod p)$$

25 où $\oplus$ est la fonction OU exclusive et H est une fonction d'adressage calculée ;
 la partie de confiance (TA) déchiffrant uniquement le message, ou émettant uniquement le message déchiffré, après exécution de ladite au moins une action avec une conclusion satisfaisante.

30 11. Procédé selon la revendication 10, dans lequel:

35 ■ le destinataire (B), avant de transférer la valeur J à la partie de confiance (TA) pour déchiffrement, la soumet à une opération de dissimulation modulo-p au moyen d'un facteur k où k est un nombre aléatoire secret ; et
 ■ la partie de confiance (TA) renvoie le message déchiffré, mais toujours dissimulé, au destinataire (B) à condition que ladite au moins une action ait été exécutée avec une conclusion satisfaisante, le destinataire (B) annulant sur ce la dissimulation pour récupérer le message.

40 12. Procédé selon la revendication 1, dans lequel ladite au moins une action comprend une étape consistant à vérifier qu'une condition a été satisfaite.

13. Procédé selon la revendication 1, dans lequel ladite au moins une action comprend une vérification concernant l'identité du destinataire.

45 14. Procédé cryptographique, dans lequel une partie de confiance (TA) avec une valeur secrète x et des paramètres publics p et g, effectue au moins les étapes consistant à :

recevoir des valeurs h et J, et une chaîne de condition STR provenant d'un expéditeur (A) de message, la chaîne de condition comprenant au moins une condition qui doit être vérifiée par la partie de confiance (TA) ;
 50 calculer :

$$z \leftarrow \#(\text{STR}), \text{ où } \# \text{ est une fonction d'adressage calculé;}$$

calculer:

55

$$f^{-1}(J, h^{z \cdot x})$$

5 où $f^{-1}()$ inverse une opération réversible $f()$, qui permet de produire un résultat qui correspond à un message déchiffré m lorsque:

10 la valeur reçue de h correspond à $g^r \bmod p$ où r est une valeur secrète appartenant à l'expéditeur (A), et la valeur reçue de J correspond à $f(g^{r \cdot x \cdot z}, m)$;
la partie de confiance (TA) calculant uniquement ledit résultat, ou émettant uniquement le résultat, après confirmation que ladite au moins une condition contenue dans la chaîne a été satisfaite.

15 15. Procédé selon la revendication 14, dans lequel $f^{-1}()$ correspond au calcul de :

$$j / h^{z \cdot x} \bmod p$$

20 le résultat étant le message m lorsque la valeur reçue de J est : $(g^{r \cdot x \cdot z}) * m \bmod p$.

16. Procédé selon la revendication 14 dans lequel $f^{-1}()$ correspond au calcul de :

$$J \oplus H(h^{z \cdot x} \bmod p)$$

25 où H est une fonction d'adressage calculée prédéterminée, le résultat étant le message m lorsque la valeur reçue de J est : $m \oplus H(g^{r \cdot x \cdot z}) \bmod p$.

30 17. Procédé selon la revendication 14, dans lequel la valeur reçue de J est une valeur dissimulée moyennant quoi ledit résultat est un résultat dissimulé.

35 18. Appareil cryptographique comprenant des première, deuxième et troisième entités de calcul, la première entité de calcul (A) comprenant:

- un agencement d'entrée destiné à recevoir une clé publique pour laquelle il existe une clé privée correspondante détenue par la deuxième entité de calcul (TA),
- un agencement de traitement de clé agencé de façon à modifier la clé publique par élévation à une puissance d'au moins un élément de la clé publique reçue en utilisant comme exposant un adressage calculé d'une chaîne (STR), cette chaîne comprenant des informations concernant au moins une action qui doit être entreprise par la deuxième entité de calcul (TA),
- un agencement de chiffrement destiné à chiffrer un message au moyen de la clé publique modifiée ; et
- un agencement de sortie destiné à sortir le message chiffré et ladite chaîne ;

45 la troisième entité de calcul (B) étant agencée de façon à recevoir le message chiffré et la chaîne et à les transmettre à la deuxième entité de calcul (TA), et la deuxième entité de calcul (TA) étant agencée de façon à recevoir un message et la chaîne, pour utiliser la chaîne afin de modifier sa clé privée pour compléter la clé publique modifiée, et pour déchiffrer le message au moyen de la clé privée modifiée, la deuxième entité de calcul (TA) étant agencée pour déchiffrer uniquement le message ; ou émettre uniquement le message déchiffré, après exécution de ladite au moins une action avec une conclusion satisfaisante.

50 19. Appareil selon la revendication 18, dans lequel la clé publique reçue comprend des éléments p , g et y , l'élément y correspondant à $g^x \bmod p$, où x est une clé privée appartenant à la deuxième entité de calcul (TA), l'agencement de traitement de clé de la première entité de calcul (A) étant agencé de façon à modifier la clé publique reçue en effectuant une élévation à une puissance modulo- p de l'élément y au moyen de l'adressage calculé de ladite chaîne (STR) en tant qu'exposant.

20. Appareil selon la revendication 19, dans lequel la deuxième entité de calcul (TA) est agencée de façon à modifier sa clé privée, par rapport à une utilisation en liaison avec la clé publique modifiée, par une opération équivalant à une multiplication de sa clé privée par l'adressage calculé de la chaîne (STR).

21. Appareil selon la revendication 19, dans lequel l'agencement de chiffrement de la première entité de calcul (A) est agencé de façon à chiffrer le message m en effectuant une élévation à une puissance modulo-p de l'élément de clé publique modifiée au moyen d'une valeur secrète r en tant qu'exposant, puis en combinant le résultat et le message m au moyen d'une opération réversible modulo-p pour former une valeur J ; l'agencement de sortie de la première entité de calcul (A) étant agencé de façon à sortir la valeur J et une valeur h correspondant à $g^r \bmod p$.

22. Appareil selon la revendication 21, dans lequel l'agencement de traitement de clé et l'agencement de chiffrement de la première entité de calcul (A) sont intégrés et agencés de sorte que les élévations à une puissance concernant une clé publique effectuées par ces deux agencements sont effectués ensemble comme une seule opération d'élévation à une puissance.

23. Appareil selon la revendication 21, dans lequel l'agencement de chiffrement est agencé de façon à exécuter ladite opération réversible par multiplication du message par ledit résultat de l'élévation à une puissance de l'élément de clé publique modifiée au moyen de la valeur secrète r.

24. Appareil selon la revendication 23, dans lequel la deuxième entité de calcul (TA) est agencée de façon à déchiffrer le message chiffré par calcul d'une valeur z en tant qu'adressage calculé de ladite chaîne (STR) puis calcul de :

$$J / h^{z \cdot x} \bmod p$$

25. Appareil selon la revendication 24, dans lequel la troisième entité de calcul (B) est agencée de façon à recevoir la valeur J et à la soumettre à une opération de dissimulation modulo-p au moyen d'un facteur k où k est un nombre aléatoire secret, avant de transférer la valeur dissimulée J à la deuxième entité de calcul (TA) ; la deuxième entité de calcul étant agencée de façon à exécuter un déchiffrement de message et à retourner le message déchiffré, mais toujours dissimulé, à la troisième entité de calcul (B) à condition que ladite au moins une action ait été exécutée avec une conclusion satisfaisante, et la troisième entité de calcul (B) étant en outre agencée de façon à recevoir le message déchiffré, mais toujours dissimulé, et à annuler la dissimulation pour récupérer le message.

26. Appareil selon la revendication 21, dans lequel l'agencement de chiffrement est agencé de façon à exécuter ladite opération réversible en effectuant une combinaison OU exclusive du message avec un adressage calculé dudit résultat de l'élévation à une puissance de l'élément de clé publique modifiée au moyen de la valeur secrète r.

27. Appareil selon la revendication 26, dans lequel la deuxième entité de calcul (TA) est agencée de façon à déchiffrer le message chiffré par calcul d'une valeur z en tant qu'adressage calculé de ladite chaîne (STR) puis calcul de :

$$J \oplus H(h^{z \cdot x} \bmod p)$$

où $\oplus$ est la fonction OU exclusive et H est une fonction d'adressage calculée.

28. Appareil selon la revendication 27, dans lequel la troisième entité de calcul (B) est agencée de façon à recevoir la valeur J et à la soumettre à une opération de dissimulation modulo-p au moyen d'un facteur k où k est un nombre aléatoire secret, avant de transférer la valeur dissimulée J à la deuxième entité de calcul (TA) ; la deuxième entité de calcul étant agencée de façon à exécuter un déchiffrement de message et à retourner le message déchiffré, mais toujours dissimulé, à la troisième entité de calcul (B) à condition que ladite au moins une action ait été exécutée avec une conclusion satisfaisante ; et la troisième entité de calcul étant (B) en outre agencée de façon à recevoir le message déchiffré, mais toujours dissimulé, et à annuler la dissimulation pour récupérer le message.

29. Entité de partie de confiance (TA) comprenant :

un magasin de données destiné à stocker une valeur secrète x et des paramètres publics p et g ;

un agencement d'entrée destiné à recevoir des valeurs h et j et une chaîne de condition STR provenant d'un expéditeur (A) de message, la chaîne de condition comprenant au moins une condition qui doit être vérifiée par la partie de confiance ;
un agencement de traitement agencé de façon à calculer:

$z \leftarrow \#(\text{STR})$, où # est une fonction d'adressage calculé ; et $f^1(J, h^{z \cdot x})$

où $f^1()$ inverse une opération réversible $f()$, qui permet de produire un résultat qui correspond à un message déchiffré m lorsque:

la valeur reçue de h correspond à $g^r \bmod p$ où r est une valeur secrète appartenant à l'expéditeur, et la valeur reçue de J correspond à $f(g^{r \cdot x \cdot z}, m)$;

un agencement de sortie destiné à sortir ledit résultat ; et

un agencement de contrôle agencé de façon à vérifier que ladite au moins une condition contenue dans la chaîne STR a été satisfaite, et à permettre uniquement à l'agencement de traitement de calculer ledit résultat, ou à permettre uniquement audit agencement de sortie de sortir ledit résultat, où ladite au moins une condition a été satisfaite.

30. Entité de partie de confiance (TA) selon la revendication 29, dans laquelle $f^1()$ correspond au calcul de :

$$J / h^{z \cdot x} \bmod p$$

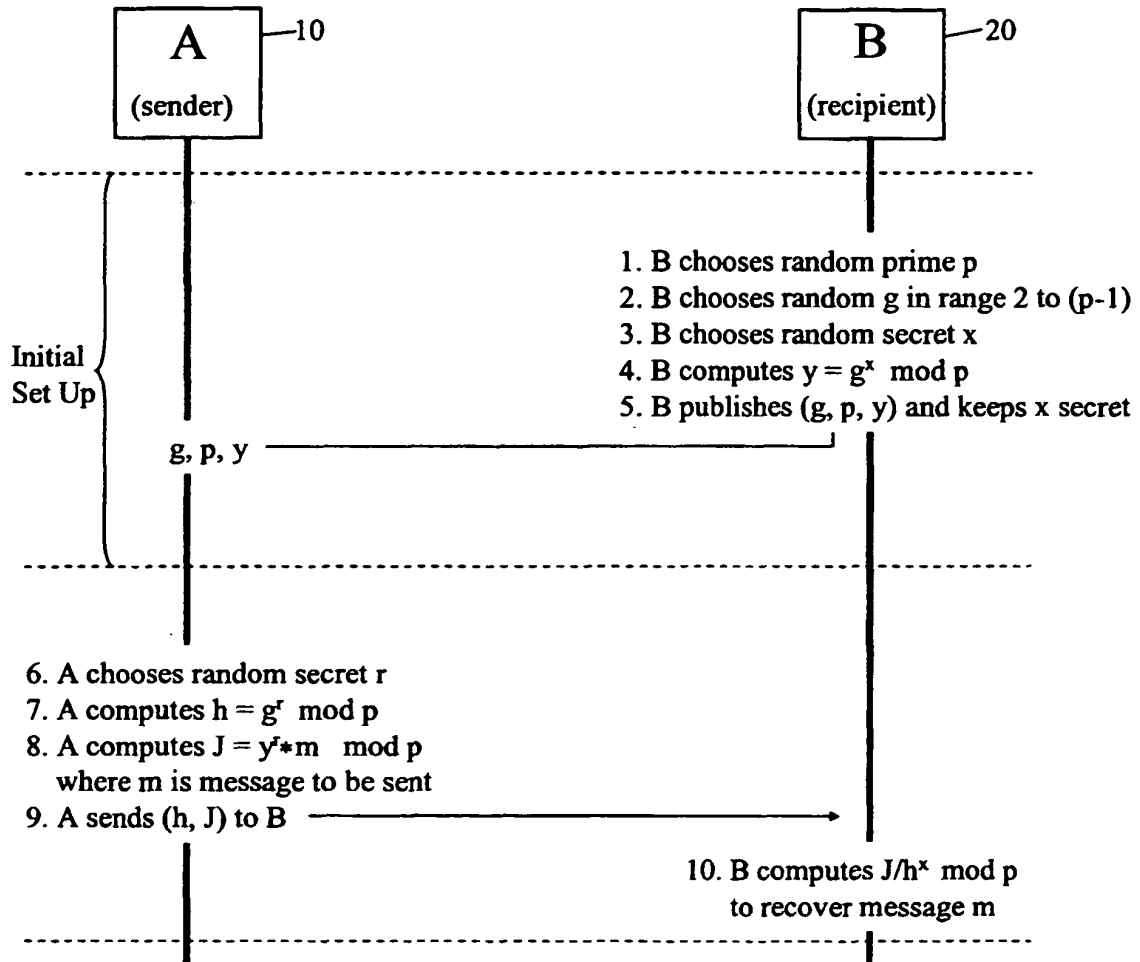
le résultat étant le message m lorsque la valeur reçue de J est : $(g^{r \cdot x \cdot z}) * m \bmod p$.

31. Entité de partie de confiance (TA) selon la revendication 29, dans laquelle $f^1()$ correspond au calcul de :

$$J \oplus H(h^{z \cdot x} \bmod p)$$

où H est une fonction d'adressage calculé prédéterminée, le résultat étant le message m lorsque la valeur reçue de J est : $m \oplus H(g^{r \cdot x \cdot z}) \bmod p$.

32. Entité de partie de confiance (TA) selon la revendication 29, dans laquelle la valeur reçue de J est une valeur dissimulée moyennant quoi ledit résultat est un résultat dissimulé.



Elgamal Encryption/Decryption

Figure 1
(Prior Art)

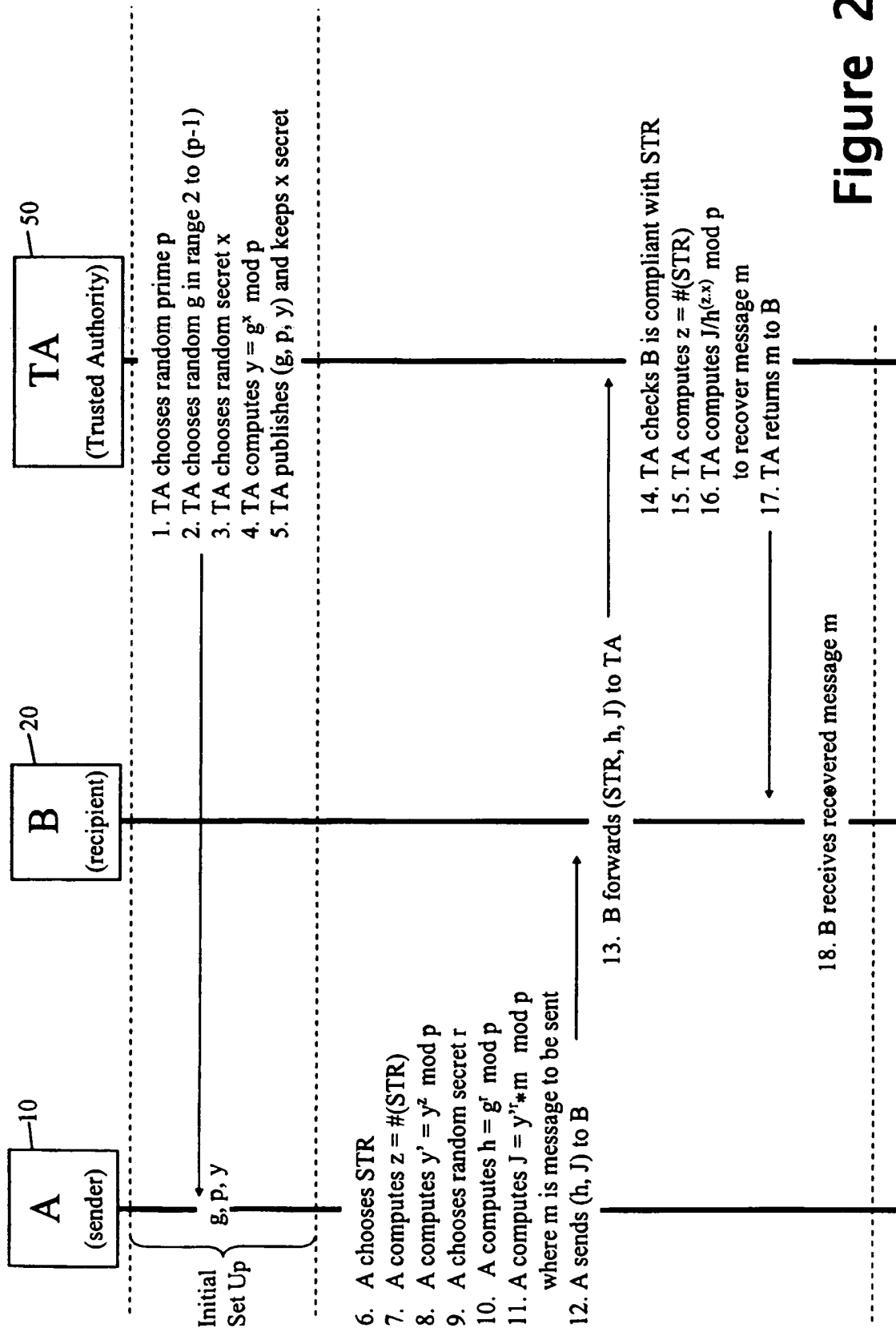


Figure 2

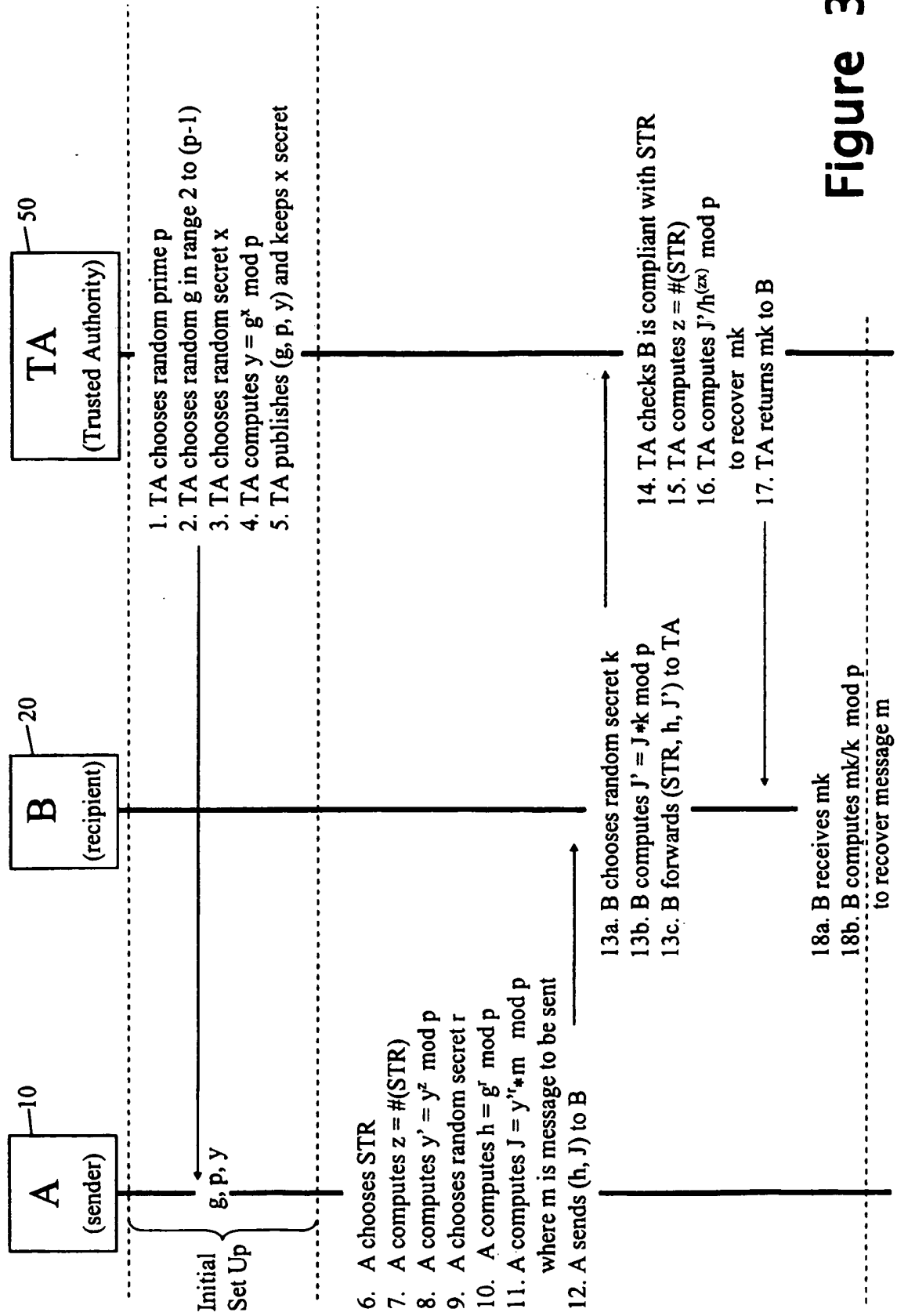


Figure 3

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 6275936 B [0004]
- WO 03063410 A [0005]

Non-patent literature cited in the description

- An identity based encryption scheme based on quadratic residues. **C. COCKS**. Proceedings of the 8th IMA International Conference on Cryptography and Coding. Springer-Verlag, 2001, vol. 2260, 360-363 [0003]
- Identity-based Encryption from the Weil Pairing. **D. BONEH ; M. FRANKLIN**. Advances in Cryptology - CRYPTO 2001, LNCS. Springer-Verlag, 2001, vol. 2139, 213-229 [0003]
- **D. BONEH ; X. DING ; G. TSUDIK**. Identity based encryption using mediated RSA. *3rd Workshop on Information Security Application*, August 2002 [0003]
- A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, July 1985, vol. IT-31 (4) [0008]